U.S. Department of Commerce
National Institute of Standards and Technology
(NIST)

Privacy Impact Assessment
for the
172-01 Human Resources System

Reviewed by: Susannah Schiller, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

□ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CATRINA PURVIS Digitally signed by CATRINA PURVIS
Date: 2020.09.30 21:47:00 -04'00' 09/30/2020

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
National Institute of Standards and Technology (NIST)

Unique Project Identifier: 172-01

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) Whether it is a general support system, major application, or other type of system
(b) System location
(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
(d) The way the system operates to achieve the purpose(s) identified in Section 4
(e) How information in the system is retrieved by the user
(f) How information is transmitted to and from the system
(g) Any information sharing conducted by the system
(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

The Office of Human Resource Management (OHRM) is responsible for planning, developing, administering, and evaluating the human resources management programs of NIST and NTIS. This enables NIST to acquire and manage a dedicated, diverse, motivated, and highly qualified workforce to accomplish its mission and achieve its goals, while ensuring compliance with pertinent Federal, Office of Personnel Management, Office of Management and Budget, and Department of Labor, policy and administrative mandates.

a. Whether it is a general support system, major application, or other type of system

The Human Resource System is a general support system.

b. System location

The GRB component is a commercially hosted application located in Virginia. The HRSTAT component stores data in Florida and Virginia facilities within the continental United States. The remaining components are located at the NIST Gaithersburg, Maryland, and Boulder, Colorado, facilities within the continental United States.

c. Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

The Performance System component shares information with the USDA National Finance Center (NFC) (for payroll processing).

d. The way the system operates to achieve the purpose(s) identified in Section 4

- **Automated Reduction in Force (ARIF): Automates the reduction-in-force process for Human Resources staff from the selection of position(s) to be abolished, to the close of the case.**
- **Performance System (Pay for Performance/General Workforce System): Provides the functionality for Human Resources staff, management, and administrative staff to record, document and report the annual employee performance rating, performance increase, bonus payout, and calculate the annual comparability increase. (ACI) for employees. Transmits updated data to the U.S. Department of Agriculture's (USDA) National Finance Center (NFC), which is the Department of Commerce's Payroll System of Record.**
- **Human Resource Arrival/Departure System (HRADS): Processes Entrance on Duty (EOD) and Departures, and automatically notifies other internal organizations of staffing changes.**
- **Government Retirement Benefits (GRB): Commercially hosted application that is used to perform employee retirement calculations based on salary and years of service. Upon an employee's request, authorized OHRM staff input the employee information into the system to perform the calculations.**
- **HR STAT: Used to initiate and submit all Human Resources (HR) service requests to include completion and submission of HR forms, personnel action requests, and other HR requests.**

e. How information in the system is retrieved by the user

Information in the components is not directly accessible by the user. Prior to employment, individuals may update their information directly with Human Resources. After the initial Human Resources hiring process, employees have opportunity to review/update their information using the National Finance Center (NFC) Employee Personal Page (EPP).

f. How information is transmitted to and from the system

The components of the system are only accessible on government issued computers through encrypted transmissions and are protected by multiple layers of firewalls. Each of the components permit assigning roles based on least privilege.

g. Any information sharing conducted by the system

The Performance System component shares information with the USDA National Finance Center (NFC) (for payroll processing).

h. *The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*

National Institute of Standards and Technology Authorization Act of 2010 (Public Law 111-358, Title IV);

5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107;

5 U.S.C. 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 3309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533, and Executive Order 9397.

i. *The Federal Information Processing Standards (FIPS) 199 security impact category for the system is* **Moderate.**

Section 1: Status of the Information System

1.1 The status of this information system:

This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017)

Changes That Create New Privacy Risks (CTCNPR)
Other changes that create new privacy risks:

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated.

Identifying Numbers (IN)
Social Security
Other identifying numbers:
Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:
SSNs are required to process Human Resource transactions beginning with the recruitment of an employee and continuing until their separation from the federal government. The SSNs are also utilized for calculating the benefits within the GRB.

General Personal Data (GPD)
Name **Maiden Name** **Alias** **Gender** **Age** **Race/Ethnicity** **Date of Birth**

Place of Birth **Home Address** **Telephone Number** **Email Address** **Education** **Military Service** **Mother's Maiden Name**
Other general personal data:

Work-Related Data (WRD)
Occupation **Job Title** **Work Address** **Work Telephone Number** **Work Email Address** **Salary** **Work History** **Business Associates**
Other work-related data:

Distinguishing Features/Biometrics (DFB)
Other distinguishing features/biometrics:

System Administration/Audit Data (SAAD)
User ID **IP Address** **Date/Time of Access**
Other system administration/audit data:

Other Information

2.2 Indicate sources of the PII/BII in the system.

Directly from Individual about Whom the Information Pertains
In Person **Hard Copy - Mail/Fax** **Online**
Other:

Government Sources
Within the Bureau **Other DOC Bureaus** **Other Federal Agencies**
Other:

Non-government Sources
Other:

2.3 Describe how the accuracy of the information in the system is ensured.

Information in the components is not directly accessible by the user. Prior to employment, individuals may update their information directly with Human Resources. After the initial Human Resources hiring process, employees have opportunity to review/update their information using the National Finance Center (NFC) Employee Personal Page (EPP).

2.4 Is the information covered by the Paperwork Reduction Act?

No, the information is not covered by the Paperwork Reduction Act.
The OMB control number and the agency number for the collection:

2.5 Is there any technology used that contain PII/BII in ways that have not been previously deployed?

Yes

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)
Personal Identity Verification (PIV) Cards
Other:

Section 3: System Supported Activities

3.1 Are there any IT system supported activities which raise privacy risks/concerns?

No

The IT system supported activities which raise privacy risks/concerns.

Activities
Other:

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated.

Purpose
To improve Federal services online **For administering human resources programs**
Other:

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

1. **The Automated Reduction in Force (ARIF) automates the reduction-in-force process from the selection of position(s) to be abolished, to the close of the case.**
2. **The Performance System (Pay for Performance/General Workforce System) administers recommended performance ratings/scores, increases, and bonuses, allowing generation of pay charts and comparability increase for employees.**
3. **The Human Resource Arrival/Departure System (HRADS) is used to process Entrance on Duty (EOD) and Departures and automatically notifies other internal organizations of staffing changes.**
4. **Government Retirement Benefits (GRB) is a commercially hosted application that is used to perform employee retirement calculations based on salary and years of service. Upon an employee's request, authorized OHRM staff input the employee information into the system to perform the calculations.**
5. **HR STAT is used to initiate and submit all Human Resource (HR) service requests to include completion and submission of HR forms, personnel action requests, and other HR requests.**
6. **The Attachment Application (NIST 183-01, Applications System Division (ASD) – Moderate Applications) workflow allows upload of attachments. The application is used as a temporary digital repository to collect forms and documents that are needed in support of prospective and current federal employees. Once documents are finalized, the forms are manually uploaded into Office of Personnel Management's systems, and purged from the Attachment Application.**

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Potential threats to privacy include the insider threat (e.g., authorized users misusing data or authorized user inadvertently combining multiple data sets resulting in aggregation of personal data).

Information collected is directly from the employee and is limited to only that which is needed for the service. Mitigating controls include employing and monitoring administrative access, training for administrators, and assurance of compliance to records management schedules.

Section 6: Information Sharing and Access

6.1 Will the PII/BII in the system be shared?

Yes, the PII/BII in the system will be shared

The recipients the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared.

Bulk Transfer - Federal agencies
Case-by-Case - DOC bureaus

Case-by-Case - Federal Agencies **Direct Access - Within the bureau**
Other:

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII.
The name of the IT system and description of the technical controls which prevent PII/BII leakage:
The Performance System component pushes data to the USDA National Finance Center and is authorized to do so via an Interconnection Security Agreement. **The NIST hosted Attachment Application (NIST 183-01, Applications System Division (ASD) – Moderate Applications) is a portal for storing HR documents that are attached to customer service requests for personnel actions. Customer service requests are initiated, stored, tracked, and managed from the NIST ServiceNow Application (188-01 NIST Platform Services System).**

6.3 Identify the class of users who will have access to the IT system and the PII/BII.

Class of Users
Government Employees
Other:

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system.

Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9. **Yes, notice is provided by a Privacy Act statement and/or privacy policy.**
The Privacy Act statement and/or privacy policy can be found at:
The Privacy Act Statement and/or privacy policy can be found at: https://www.nist.gov/privacy-policy. A government warning banner is displayed when logging into the applications.
The reason why notice is/is not provided:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

Yes, individuals have an opportunity to decline to provide PII/BII. **No, individuals do not have an opportunity to decline to provide PII/BII.**
The reason why individuals can/cannot decline to provide PII/BII:
Yes:

For GRB component, individuals have the opportunity to decline to provide PII/BII. In doing so, their retirement benefits will not be calculated. **No:** **For the ARIF, Performance System, and HRADS components, employees may not decline after the initial Human Resources hiring process.**

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

No, individuals do not have an opportunity to consent to particular uses of their PII/BII.
The reason why individuals can/cannot consent to particular uses of their PII/BII:
Individuals are not given an opportunity to give consent after the initial Human Resources hiring process.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

Yes, individuals have an opportunity to review/update PII/BII pertaining to them.
The reason why individuals can/cannot review/update PII/BII:
Prior to employment, individuals may update their information directly with Human Resources. After the initial Human Resources hiring process, employees have opportunity to review/update their information using the National Finance Center (NFC) Employee Personal Page (EPP).

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system.

All users signed a confidentiality agreement or non-disclosure agreement. **All users are subject to a Code of Conduct that includes the requirement for confidentiality.** **Staff (employees and contractors) received training on privacy and confidentiality policies and practices.** **Access to the PII/BII is restricted to authorized personnel only.** **Access to the PII/BII is being monitored, tracked, or recorded.** **The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements.** **The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.** **NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).** **A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.**

Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
Reason why access to the PII/BII is being monitored, tracked, or recorded:
Access logs are kept and reviewed for anomalies.
The information is secured in accordance with FISMA requirements.
Is this a new system? No **Below is the date of the most recent Assessment and Authorization (A&A).** **04/30/2020**
Other administrative and technological controls for the system:

8.2 General description of the technologies used to protect PII/BII on the IT system. *(Includes data encryption in transit and/or at rest, if applicable).*

The components of the system are accessible on internal NIST networks protected by multiple layers of firewalls. Unauthorized use of the system is restricted by user authentication. Access logs are kept and reviewed for anomalies. For each component, PII is transferred in a secure fashion, and data-at-rest is encrypted. To guard against the interception of communication over the network, the components use the Transport Layer Security (TLS) protocol which encrypts communications between users' web browsers and the web server. Data that flows between the web server and the database server is secured through encrypted communication.

For the Performance System component, data shared with the National Finance Center uses FIPS 140-2 encrypted virtual private network technologies.

For the GRB application, user authentication and firewall administration is administered by the company.

For the Attachment Application (NIST 183-01, Applications System Division (ASD) – Moderate Applications), data is scanned for viruses upon upload.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?
Yes

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

Yes, this system is covered by an existing system of records notice (SORN).
SORN name, number, and link:
NIST-1 **NIST Associates** **Commerce/DEPT-1** **Attendance, Leave, and Payroll of Employees and Certain Other Persons** **Commerce/DEPT-18**

Employee Personnel Files NOT Covered by Notices of Other Agencies **OPM/GOVT-1** **General Personnel Records** **OPM/GOVT-2** **Employee Performance File Systems Records** **OPM/GOVT-3** **Records of Adverse Actions, Performance Based Reductions in Grade and Removal Actions, and Terminations of Probationers** **OPM/GOVT-5** **Recruiting, Examining, and Placement Records** **OPM/GOVT-6** **Personnel Research and Test Validation Records** **OPM/GOVT-7** **Applicant Race, Sex, National Origin, and Disability Status Records**
SORN submission date to the Department:

Section 10: Retention of Information

10.1 Are these records are covered by an approved records control schedule and monitored for compliance?

Yes, there is an approved record control schedule.
Name of the record control schedule:
General Records Schedule 1.0 **General Records Schedule 2.0 Human Resources** **General Records Schedule 3.0 Technology**
The stage in which the project is in developing and submitting a records control schedule:
Yes, retention is monitored for compliance to the schedule.
Reason why retention is not monitored for compliance to the schedule:

10.2 Indicate the disposal method of the PII/BII.

Disposal
Shredding **Deleting**
Other disposal method of the PII/BII:

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

11.2 The factors that were used to determine the above PII confidentiality impact levels.

Factors that were used to determine the above PII confidentiality impact levels	Explanation
Identifiability **Quantity of PII** **Data Field Sensitivity** **Obligation to Protect Confidentiality** **Access to and Location of PII**	**Identifiability-The data types that are collected and maintained can be used to identify specific individuals.** **Quantity of PII-The quantity of the PII that is collected and maintained pertains to all federal employees, past and present.** **Data Field Sensitivity-Personal identification numbers are used to identify individuals.** **Obligation to Protect Confidentiality-The organization is legally obligated to protect the PII within the application.** **Access to and Location of PII-The information system is comprised of several applications that store and process PII.**

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Potential threats to privacy include the insider threat (e.g., authorized users misusing data or authorized user inadvertently combining multiple data sets resulting in aggregation of personal data).

Information collected is directly from the employee and is limited to only that which is needed for the service. Mitigating controls include employing and monitoring administrative access, training for administrators, and assurance of compliance to records management schedules.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

No, the conduct of this PIA does not result in required business process changes.
Explanation

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

No, the conduct of this PIA does not result in any required technology changes.
Explanation